



UNITED STATES PATENT AND TRADEMARK OFFICE

98

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/773,716

01/31/2001

Masayuki Chatani

375.07.01

7005

25920

7590

12/14/2005

MARTINE PENILLA & GENCARELLA, LLP
710 LAKEWAY DRIVE
SUITE 200
SUNNYVALE, CA 94085

EXAMINER

COLIN, CARL G

ART UNIT

PAPER NUMBER

2136

DATE MAILED: 12/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/773,716	Applicant(s) CHATANI ET AL.	
	Examiner Carl Colin	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03 October 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 88-109 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 88-109 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 31 January 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
 If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) ☐ All b) ☐ Some * c) ☐ None of:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
 * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
 a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) <u>see att</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 10/3/2005, applicant amends claims 88, 94, 100, and 106. The following claims 88-109 are presented for examination.

2. Applicant's arguments, pages 11-13, filed on 10/3/2005, with respect to the rejection of claims 88-109 have been fully considered but they are not persuasive. Applicant states that claim 58 has been amended to recite that double encryption is asymmetric because Uranaka discloses double encryption that is symmetric. However, Applicant by this amendment has not overcome the rejection of claim 58 as combined and as rejected in the Office Action. Applicant also argues that Uranaka does not disclose generating keys using user information because if the user key is recorded on the DVD at the time of selling the DVD, it cannot be generated.

Examiner respectfully disagrees. Column 14, lines 25-37 discloses recording specific public key on the DVD and each public key is assigned to specific family member. See also column 14, lines 59-67 and column 7, lines 58-67). Uranaka even discloses user specific information is recorded on the DVD for authentication. Uranaka discloses a system for permitting only an authentic user user who have legally obtained charged information to use charged information. (see column 2, lines 8-18 and lines 55-67). As further evidence, US Patent 5,490,216 clearly shows that keys may be generated during user registration using user information from a specific user. Applicant's Disclosure filed 8/1/2005 also shows evidence that key pairs may be generated

Art Unit: 2136

based on user's information. Upon further consideration Examiner maintains the rejection of claims 21-47 in view of the same references.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3.1 **Claims 88-109** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,470,085 to **Uranaka et al** in view of Non-Patent Literature Bruce **Schneier**; "Applied Cryptography", 1996; John Wiley & Sons; Second edition; Pages 31-32, 39, 176-177, and 357-360.

3.2 **As per claims 88-89, 94, 96-101, 106, and 108-109, Uranaka et al** substantially discloses a method for enabling access to a software product, communication to enable the access to the software product being between a user computer and a server computer, the user

Art Unit: 2136

computer executing program instructions to enable the method (column 4, lines 44-65), comprising: receiving user information from the user computer (column 3, lines 30-45);

Uranaka et al discloses generating server key pair at the server based on user's information that meets the recitation of user key pair (column 8, lines 34-41). Column 14, lines 25-37 discloses recording specific public key on the DVD and each public key is assigned to specific family member that meets the recitation of user key pair generated using information from a specific user; this is well known as disclosed in US Patents 6,195,432 and Korean Application number KR 1998-033266 and JP9-244886 in Applicant's disclosure filed on 8/1/05 and US Patent 5,490,216, in order to limit control of usage only to specific individual members as suggested by **Uranaka et al**. **Uranaka et al** discloses the server public key is obtained by the user (column 19, lines 2-10 and column 15, lines 55-67). **Uranaka et al** further discloses generating user key pair at the user computer that meets the recitation of console key pair and sending the user public key to the server to use for double encryption (column 7, lines 1-9; column 11, lines 13-20 and column 22, lines 26-36) and suggests that data transmitting with the service request can be encrypted (column 18, lines 61 through column 19, line 2); receiving a title ID from the user computer, the title ID identifying the software product for which access is desired, the title ID being encrypted by the user public key (column 22, lines 25-27 and column 18, lines 61 through column 19, line 2; and column 24, lines 30-40); retrieving a title private key based on the title ID received, the title private key being double encrypted asymmetrically by the server computer using the console public key and the user private key, use of the console public key created at the user computer defining a first layer of encryption, use of the user private key created at the server computer defining a second layer of encryption, the title private key and the

Art Unit: 2136

title public key defining a title key pair (column 22, lines 29-36); and forwarding the double encrypted title private key to the user computer so that the user computer can use the title private key to decrypt the software product encrypted by using the title public key (column 22, lines 36-50 and column 14, line 59 through column 15, line 21).

Uranaka et al discloses the invention as a whole comprising of exchanging at least three key pairs between the client and the server; suggests that data transmitting with the service request can be encrypted (column 18, lines 61 through column 19, line 2); and discloses the double encryption of a title private key K_v using a key generating by the user P_{ku} and a key generating by the server (R). **Uranaka et al** discloses double encryption and the key (K_v) sent by the server is encrypted by two keys (one key from the server and one key from the user): a server key R and encrypted by a public key P_{ku} (column 15, lines 1-4). **Uranaka et al** even discloses signing the double encryption key with a key pair (column 15, lines 55-67). The decryption steps in the claims, for instance in claims 96-97 are disclosed in **Uranaka et al** because they are just the reverse of the encryption steps cited above as known in the art of cryptography. The difference between **Uranaka et al** and the claimed invention is that the key (R) is a shared key.

It is well known that using key pair provides more security than a shared key. **Schneier** also discloses multiple encryption and suggests making sure that multiple keys are different and independent to benefit from multiple encryption. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Uranaka et al** to change the symmetric random key to an asymmetric key in order to provide more security as taught by **Schneier**. This modification would have been obvious to one skilled in the

Art Unit: 2136

art to use the random key as a key pair instead of using it as a shared key because asymmetric cryptography is more secure than symmetric cryptography so it will provide more security because key may also be compromised during transmission and using different key that is known only to one party may benefit in security as suggested by **Schneier**.

As per claims 90, 95, 102, and 107, Uranaka et al discloses receiving purchase information from the user computer (column 12, lines 5-25); creating an electronic token based on the purchase information; and forwarding to the user computer, the electronic token that permits use of the decrypted software product in a restricted manner (column 12, lines 40-67).

As per claims 91 and 103, Uranaka et al discloses wherein the initiating of the access to the server computer is carried out by forwarding user information specific to the user computer to the server computer (column 5, lines 10-42; column 7, lines 57-67; and column 8, lines 34-41).

As per claims 92 and 104, Uranaka et al discloses different embodiments or alternatives of creating key pairs at the server based on user information (column 8, lines 34-42 and column 15, lines 21-67).

As per claims 93 and 105, Uranaka et al discloses wherein the console key pair is created by the user computer by using hardware identification means (column 18, lines 41-53; column 22, lines 26-36).

Conclusion

4. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

4.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

Art Unit: 2136

applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Carl Colin

Patent Examiner

December 9, 2005

Carl
Primary Examiner
AU2131
12/12/05